THE DISTRIBUTION OF IRREDUCIBLE POLYNOMIALS IN SEVERAL INDETERMINATES[1]

BY

L. CARLITZ

1. It is well known that the number of normalized irreducible polynomials of degree m in a single indeterminate, with coefficients in $GF(q)$, is given by

$$\psi_1(m) = (1/m) \sum_{rs=m} \mu(r) q^s, \tag{1}$$

where $\mu(r)$ is the Möbius function. It follows from (1) that, if q is fixed,

$$\psi_1(m) \sim (1/m) q^m \qquad (m \to \infty). \tag{2}$$

For the case of irreducible polynomials in several indeterminates, with coefficients in $GF(q)$, no explicit formula like (1) seems to be available. We shall show, however, that an asymptotic formula for the number of irreducibles can be obtained easily. This formula differs from (2) in one important respect. When the number of indeterminates is greater than one we find that almost all polynomials are irreducible.

2. By the degree of a polynomial $M(x_1, \cdots, x_k)$ will be understood the *total* degree. We assume that the polynomials have been normalized by selecting one polynomial from each equivalence class with respect to multiplication by nonzero constants.

Let $f(m) = f_k(m)$ denote the number of normalized polynomials of degree m in k indeterminates. Let $\psi_k(m)$ denote the number of normalized irreducible polynomials of degree m, and put

$$g(m) = g_k(m) = \sum_{r \mid m} r\psi_k(r). \tag{3}$$

As a special case of a slightly more general theorem [1, p. 273] we have

$$mf_k(m) = \sum_{s=1}^{m} g_k(s) f_k(m - s). \tag{4}$$

For completeness we give a brief proof of (4). Put

$$F_k(m) = \prod_{\deg M=m} M, \qquad \Theta_k(m) = \prod_{\deg P=m} P, \tag{5}$$

so that $F_k(m)$ is the product of the normalized polynomials of degree m in k indeterminates and $\Theta_k(m)$ is the product of the normalized irreducible polynomials. If

$$M = P^e A \qquad (P \nmid A),$$

where $\deg P = s$, it follows from the first of (5) that

$$F_k(m) = \prod_{P,e} P^{e\phi_{m-es}(P)}, \tag{6}$$

Received December 20, 1961.

[1] Supported in part by a National Science Foundation grant.

where $\phi_j(P)$ denotes the number of normalized polynomials of degree j not divisible by P and the product is over all P, e such that $es \leqq m$. Since

$$\begin{aligned} \phi_j(P) &= f_k(j) && \text{if } j < s, \\ &= f_k(j) - f_k(j-s) && \text{if } j \geqq s, \end{aligned}$$

(6) becomes

$$F_k(m) = \prod_P P^w, \tag{7}$$

where

$$\begin{aligned} w &= \sum_e e\phi_{m-es}(P) \\ &= \{f_k(m-s) - f_k(m-2s)\} + 2\{f_k(m-2s) - f_k(m-3s)\} \\ &\qquad + \cdots + rf_k(m-rs) = \sum_{e=1}^r f_k(m-es), \end{aligned}$$

where $r = [m/s]$. Hence (7) implies

$$F_k(m) = \prod_{s=1}^m \{\Theta_k(s)\}^{f_k(m-s)+\cdots+f_k(m-rs)}. \tag{8}$$

Comparing the degrees of both sides of (8) we get

$$\begin{aligned} mf_k(m) &= \sum_{s=1}^m s\psi_k(s) \sum_{e=1}^r f_k(m-es) = \sum_{0<es\leqq m} s\psi_k(s) f_k(m-es) \\ &= \sum_{j=1}^m f_k(m-j) \sum_{es=j} s\psi_k(s) = \sum_{j=1}^m f_k(m-j) g_k(j), \end{aligned}$$

which proves (4).

3. It is easily verified that

$$f_k(m) = (q-1)^{-1}\left\{\exp_q\binom{m+k}{k} - \exp_q\binom{m+k-1}{k}\right\}, \tag{9}$$

where $\exp_q a = q^a$. Then it follows from (4) and (9) that

$$g_k(m) \leqq mf_k(m) \leqq m(q-1)^{-1}\exp_q\binom{m+k}{k},$$

so that

$$\begin{aligned} mf_k(m) - g_k(m) &= \sum_{s=1}^{m-1} g_k(s) f_k(m-s) \\ &\leqq m(q-1)^{-2} \sum_{s=1}^{m-1} \exp_q\binom{s+k}{k} \exp_q\binom{m-s+k}{k} \\ &\leqq 2m(q-1)^{-2} \sum_{1\leqq s\leqq m/2} \exp_q\left\{\binom{s+k}{k} + \binom{m-s+k}{k}\right\}. \end{aligned}$$

But for $2 \leqq s \leqq m/2$ and $k > 1$ we have

$$\begin{aligned} &\left\{\binom{s-1+k}{k} + \binom{m-(s-1)+k}{k}\right\} - \left\{\binom{s+k}{k} + \binom{m-s+k}{k}\right\} \\ &\qquad = \binom{m-s+k}{k-1} - \binom{s-1+k}{k-1} \geqq \binom{[m/2]+k}{k-1} - \binom{[m/2]+k-1}{k-1} \\ &\qquad = \binom{[m/2]+k-1}{k-2} \geqq 1, \end{aligned}$$

so that

$$
\begin{aligned}
mf_k(m) - g_k(m) & \\
&\leqq 2m(q-1)^{-2}\exp_q\left\{\binom{k+1}{k} + \binom{m+k-1}{k}\right\}(1+q^{-1}+q^{-2}+\cdots) \\
&= 2mq(q-1)^{-3}\exp_q\left\{\binom{k+1}{k} + \binom{m+k-1}{k}\right\} \\
&= O\left(m\exp_q\binom{m+k-1}{k}\right).
\end{aligned}
$$

Since

$$f_k(m) = (q-1)^{-1}\exp_q\binom{m+k}{k} + O\left(\exp_q\binom{m+k-1}{k}\right),$$

it follows that

$$g_k(m) = m(q-1)^{-1}\exp_q\binom{m+k}{k} + O\left(m\exp_q\binom{m+k-1}{k}\right). \tag{10}$$

But by (3) and (10)

$$m\psi_k(m) = g_k(m) + O\left(m\exp_q\binom{[m/2]+k}{k}\right),$$

which yields

$$\psi_k(m) = (q-1)^{-1}\exp_q\binom{m+k}{k} + O\left(\exp_q\binom{m+k-1}{k}\right). \tag{11}$$

We state the

THEOREM. *The number of normalized irreducible polynomials in k indeterminates, with coefficients in $GF(q)$, satisfies* (11). *In particular it follows that*

$$\psi_k(m) \sim f_k(m) \qquad (m \to \infty), \tag{12}$$

where $f_k(m)$ is the total number of normalized polynomials in k indeterminates, with coefficients in $GF(q)$.

Remark. For the number of irreducible *factorable* polynomials in k indeterminates, that is, polynomials that factor completely in some extension of $GF(q)$, (12) no longer holds (see [2]).

4. As the referee has pointed out, (12) can be proved by a crude counting argument. Indeed it is evident that the number of normalized reducible polynomials of degree m

$$\leqq \sum_{1\leqq s\leqq m/2} f_k(s)f_k(m-s) \leqq (q-1)^{-2}\sum_{1\leqq s\leqq m/2}\exp_q\left\{\binom{s+k}{k} + \binom{m-s+k}{k}\right\}.$$

But, as we have seen above, the right member

$$
\begin{aligned}
&\leqq (q-1)^{-2}\exp_q\left\{\binom{k+1}{k} + \binom{m+k-1}{k}\right\}(1+q^{-1}+q^{-2}+\cdots) \\
&= q(q-1)^{-3}\exp_q\left\{\binom{m+k}{k} - \binom{m+k-1}{k-1} + k + 1\right\} \\
&\leqq (q-1)^{-3}\exp_q\left\{-\binom{m+k-1}{k-1} + k + 3\right\} f_k(m).
\end{aligned}
$$

It follows that

$$1 - (q-1)^{-3}\exp_q\left\{-\binom{m+k-1}{k-1} + k + 3\right\} \leqq \psi_k(m)/f_k(m) \leqq 1. \tag{13}$$

For m large it is evident that the left member of (13) is very close to 1, so that (12) follows. The referee has noted that if $k > 1$, then

$$\psi_k(m)/f_k(m) \geqq \tfrac{5}{8}, \tag{14}$$

the worst case being when $k = m = q = 2$.

5. Returning to (8), we put

$$G_k(m) = \prod_{s \mid m} \Theta_k(s). \tag{15}$$

Then

$$F_k(m) = \prod_{es \leqq m} \{\Theta_k(s)\}^{f_k(m-es)} = \prod_{t=1}^{m} \{\prod_{s \mid t} \Theta_k(s)\}^{f_k(m-t)},$$

so that

$$F_k(m) = \prod_{t=1}^{m} \{G_k(t)\}^{f_k(m-t)}. \tag{16}$$

When $k = 1$, it is familiar that

$$G_1(m) = x^{q^m} - x, \tag{17}$$

but there seems to be no simple formula of this kind for $k > 1$.

If we let $L_k(m)$ denote the least common multiple of the polynomials in k indeterminates, of degree m, then it is clear that

$$\begin{aligned} L_k(m) &= \prod_{\deg P \leqq m} P^{[m/\deg P]} = \prod_{s=1}^{m} \{\prod_{\deg P = s} P\}^{[m/s]} \\ &= \prod_{s=1}^{m} \{\Theta_k(s)\}^{[m/s]} = \prod_{es \leqq m} \Theta_k(s) \\ &= \prod_{t=1}^{m} \prod_{s \mid t} \Theta_k(s). \end{aligned}$$

Therefore by (15) we get

$$L_k(m) = \prod_{t=1}^{m} G_k(t). \tag{18}$$

Since $\deg G_k(m) = g_k(m)$, it follows from (18) that

$$\deg L_k(m) = \sum_{t=1}^{m} g_k(t).$$

6. It follows from (3) that

$$m\psi_k(m) = \sum_{rs=m} \mu(r) g_k(s). \tag{19}$$

Thus when $g_k(m)$ is known, $\psi_k(m)$ can be computed explicitly.

Since $\psi_k(m)$ is integral, it follows from [1, §2] that $g_k(m)$ satisfies

$$g_k(mp^r) \equiv g_k(mp^{r-1}) \pmod{p^r} \tag{20}$$

where p is a prime and $m \geqq 1$, $r \geqq 1$.

We have also

$$g_k(m) \equiv k \pmod{q - 1}. \tag{21}$$

Indeed by (9) and (4)

$$f_k(1) = g_k(1) = q^k + q^{k-1} + \cdots + q \equiv k \pmod{q - 1},$$

so that (21) holds for $m = 1$. We assume the truth of (21) up to and including the value $m - 1$. Now by (9)

$$f_k(m) \equiv \binom{m+k}{k} - \binom{m+k-1}{k} \equiv \binom{m+k-1}{k-1} \pmod{q-1}.$$

Thus by (4) and the inductive hypothesis

$$\begin{aligned} g_k(m) &\equiv m\binom{m+k-1}{k-1} - k \sum_{s=1}^{m-1} \binom{s+k-1}{k-1} \\ &\equiv m\binom{m+k-1}{k-1} - k\binom{m+k-1}{k} + k \\ &\equiv m\binom{m+k-1}{k-1} - m\binom{m+k-1}{k-1} + k \\ &\equiv k \qquad \pmod{q-1}. \end{aligned}$$

When $k = 1$, we have

$$f_1(m) = g_1(m) = q^m. \tag{22}$$

Conversely, if

$$f_k(m) = g_k(m) \qquad (m = 1, 2, 3, \cdots), \tag{23}$$

then $k = 1$. Indeed it is enough to assume that

$$f_k(2) = g_k(2). \tag{24}$$

We have

$$f_k(1) = g_k(1) = q^k + q^{k-1} + \cdots + q.$$

Then by (4) and (24)

$$f_k(2) = (q^k + q^{k-1} + \cdots + q)^2,$$

so that by (9)

$$q^{(k+1)(k+2)/2} - q^{k+1} = (q-1)(q^k + \cdots + q)^2.$$

Put $q = p^n$; then the right member is divisible by exactly p^{2n}. It follows that $k + 1 = 2$, $k = 1$.

References

1. L. Carlitz, *An arithmetic function*, Bull. Amer. Math. Soc., vol. 43 (1937), pp. 271–276.
2. ———, *On factorable polynomials in several indeterminates*, Duke Math. J., vol. 2 (1936), pp. 660–670.

Duke University
Durham, North Carolina